desktop management guide

hp workstation xw4000
hp workstation xw6000

Document Part Number: 301201-001

October 2002

This guide provides definitions and instructions for using security and Intelligent Manageability features that are preinstalled on select models.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material. The information in this document is provided "as is" without warranty of any kind, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, and is subject to change without notice. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

⚠ **WARNING:** Text set off in this manner indicates that failure to follow directions could result in bodily harm or loss of life.

△ **CAUTION:** Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

desktop management guide
hp workstation xw4000
hp workstation xw6000
First Edition (October 2002)
Document Part Number: 301201-001

Contents

Desktop Management Guide

Desktop Management Guide

HP pioneered desktop manageability in 1995 with the introduction of the industry's first fully manageable desktop personal computers. Since then, HP has led an industry-wide effort to develop the standards and infrastructure required to effectively deploy, configure, and manage desktops, workstations, and notebook PCs. HP Intelligent Manageability provides standards-based solutions for managing and controlling desktops, workstations, and notebook PCs in a networked environment. HP works closely with leading management software solution providers in the industry to ensure compatibility between Intelligent Manageability and these products. Intelligent Manageability is an important aspect of our broad commitment to providing you with PC Lifecycle Solutions that assist you during the four phases of the desktop PC lifecycle—planning, deployment, management, and transitions.

This guide summarizes the capabilities and features of the seven key components of desktop management:

- Initial configuration and deployment
- Remote system installation
- Software updating and management
- ROM flash
- Building blocks and partners
- Asset tracking and security
- Fault notification and recovery

✎ Support for specific features described in this guide may vary by model or software version.

Initial Configuration and Deployment

Your computer comes with a preinstalled system software image. After a very brief software “unbundling” process, the computer is ready to be used.

You may prefer to replace the preinstalled software image with a customized set of system and application software. There are several methods for deploying a customized software image. They include:

- Installing additional software applications after unbundling the preinstalled software image.
- Using software deployment tools, such as Altiris eXpress, Microsoft MS Batch, or Microsoft NT Distribution Share (NTDS), to replace the preinstalled software with a customized software image.
- Using a disk cloning process to copy the contents from one hard drive to another.

The best deployment method depends on your information technology environment and processes. The PC Deployment section of the Solutions and Services Web site (http://www.compaq.com/solutions/pcsolutions) provides information to help you select the best deployment method. You will also find guides and utilities to integrate Microsoft or PXE-based deployment tools.

The *Compaq Restore* CD (or *Restore Plus!* CD), ROM-based setup, and ACPI-ready hardware provide further assistance with recovery of system software, configuration management and troubleshooting, and power management.

Remote System Installation

Remote System Installation allows you to start and set up your system using the software and configuration information located on a network server. The Remote System Installation feature is usually used as a system setup and configuration tool, and can be used for the following tasks:

- Deploying a software image on one or more new PCs.
- Formatting a hard drive.

- Installing application software or drivers.
- Updating the operating system, application software, or drivers.

To initiate Remote System Installation, press **F12** when the F12 = Network Service Boot message appears in the lower-right corner of the HP logo screen. Follow the instructions on the screen to continue the process.

HP and Altiris, Inc. have partnered to provide tools designed to make the task of corporate PC deployment and management easier and less time-consuming, ultimately lowering the total cost of ownership and making HP PCs the most manageable client PCs in the enterprise environment.

Software Updating and Management

HP provides several tools for managing and updating software on desktops and workstations—Altiris eXpress, Altiris eXpress PC Transplant Pro, Altiris eXpress HP/Compaq Client Manager, System Software Manager, Product Change Notification, and ActiveUpdate.

Altiris eXpress

HP and Altiris have extended their partnership to deliver industry-leading solutions that reduce the complexity of managing hardware and software for desktops, notebooks, handheld devices, and servers throughout their lifecycle. Altiris eXpress allows the system administrator to create and quickly deploy a customized, corporate-standard software image across one or more networked client PCs with an interface as simple to use as Windows Explorer. Altiris eXpress supports Intel’s Wired for Management and Preboot Execution Environment (PXE). Using Altiris eXpress and the Remote System Installation features of the HP computer, there is no need for the system administrator to visit each new PC individually to deploy the software image.

The Altiris eXpress solutions provide an efficient and effective way to automate existing processes and address problem areas within your IT environment. With the Altiris eXpress web-based infrastructure, you have the flexibility to manage your systems from anywhere at anytime—even from your iPAQ Pocket PC!

The Altiris eXpress solutions are modular and extensible to span the needs of workgroups to the enterprise. They integrate with other industry client management tools and provide extensions to Microsoft BackOffice/SMS.

The expanded Altiris eXpress solutions focus on four key IT areas:

- Deployment & Migration
- Software & Operations Management
- Inventory & Asset Management
- Help Desk & Problem Resolution

Within minutes of installation, Altiris eXpress is able to install a disk image containing the operating system, application software, and the Altiris eXpress client, without requiring the use of a separate boot diskette. With Altiris eXpress, the network administrator can:

- Create a new image or edit an existing image, or clone a PC on the network which may have the ideal image.
- Create any number of customized disk images for a variety of workgroups.
- Edit image files, modifying them without having to start from scratch. This is possible because Altiris eXpress stores files in its native format: NTFS, FAT16, or FAT32.
- Establish a “New PC Event,” a script that will run automatically when a new PC is added to the network. The script can, for instance, format the PC hard drive, flash the ROM BIOS, and install a full, standard software image.
- Schedule an event to run on a group of computers.

Altiris eXpress also includes easy-to-use software distribution capabilities. You can use Altiris eXpress to update operating systems and application software from a central console. When used in conjunction with System Software Manager, Altiris eXpress can also update ROM BIOS and device driver software.

For more information, visit
http://www.compaq.com/easydeploy.

Altiris eXpress PC Transplant Pro

Altiris eXpress PC Transplant Pro offers painless PC migration by preserving old settings, preferences, and data and migrating them to the new environment quickly and easily. Upgrades take minutes rather than hours or days, and the desktop and applications look and work just as your users expect.

For more information and details on how to download a fully-functional 30-day evaluation, visit http://www.compaq.com/easydeploy.

Altiris eXpress HP/Compaq Client Manager

The Altiris eXpress HP/Compaq Client Manager tightly integrates HP Intelligent Manageability technology within Altiris eXpress to provide superior hardware management capabilities for HP access devices that include:

- Detailed views of hardware inventory for asset management
- PC health check monitoring and diagnostics
- Proactive notification of changes in your hardware environment
- Web-accessible reporting of business critical details such as machines with thermal warnings, memory alerts, and more
- Remote updating of system software such as device drivers and ROM BIOS

For more information on the Altiris eXpress HP/Compaq Client Manager, visit http://www.compaq.com/easydeploy.

System Software Manager

System Software Manager (SSM) is a utility that lets you update system-level software on multiple systems simultaneously. When executed on a PC client system, SSM detects both hardware and software versions, then updates the appropriate software from a central repository, also known as a file store. Driver versions that are supported by SSM are denoted with a special icon on the driver download Web site and on the Support Software CD. To download the utility or to obtain more information on SSM, visit http://www.compaq.com/im/ssmwp.html.

Product Change Notification

PCN is the Product Change Notification program from HP that uses a secure Web site where you create custom profiles to proactively and automatically:

- Receive email notification of hardware and software changes to most commercial computers and servers.
- Receive email containing Customer Advisories for most commercial computers and servers.

The PCN Web site also allows users to search all Product Change Notifications and Customer Advisories for most commercial PCs and servers.

To learn more about PCN and create your custom profile, visit http://www.compaq.com/pcn.

ActiveUpdate

ActiveUpdate is a client-based application from HP. The ActiveUpdate client runs on your local system and uses your user-defined profile to proactively and automatically download software updates for most Compaq/HP commercial computers and servers.

To learn more about ActiveUpdate, download the application, and create your custom profile, visit http://www.compaq.com/activeupdate.

ROM Flash

Your computer comes with a reprogrammable flash ROM (read only memory). By establishing a setup password in Computer Setup (F10) Utility, you can protect the ROM from being unintentionally updated or overwritten. This is important to ensure the operating integrity of the computer. Should you need or want to upgrade your ROM, you may:

- Order an upgraded *ROMPaq*™ diskette from HP.
- Download the latest ROMPaq images from http://www.compaq.com.

⚠ **CAUTION:** For maximum ROM protection, be sure to establish a setup password. The setup password prevents unauthorized ROM upgrades. System Software Manager allows the system administrator to set the setup password on one or more PCs simultaneously. For more information, visit http://www.compaq.com/im/ssmwp.html.

Remote ROM Flash

Remote ROM Flash allows the system administrator to safely upgrade the ROM on remote HP computers directly from the centralized network management console. Enabling the system administrator to perform this task remotely, on multiple computers and personal computers, results in a consistent deployment of and greater control over HP PC ROM images over the network. It also results in greater productivity and lower total cost of ownership.

✎ Your computer must be powered on, or turned on through Remote Wakeup, to take advantage of Remote ROM Flash.

For more information on Remote ROM Flash, refer to the Altiris eXpress HP/Compaq Client Manager or System Software Manager at http://www.compaq.com/easydeploy.

FailSafe Boot Block ROM

The FailSafe Boot Block ROM allows for system recovery in the unlikely event of a ROM flash failure, for example, if a power failure were to occur during a ROM upgrade. The Boot Block is a flash-protected section of the ROM that checks for a valid system ROM flash when power to the system is turned on.

- If the system ROM is valid, the system starts normally.
- If the system ROM fails the validation check, the FailSafe Boot Block ROM provides enough support to start the system from a ROMPaq diskette, which will program the system ROM with a valid image.

When the Boot Block detects an invalid system ROM, the system sounds a series of beeps (one long and three short) and flashes the three keyboard lights (on and off two times). A Boot Block recovery mode message is displayed on the screen (some models).

To recover the system after it enters Boot Block recovery mode, complete the following steps:

1. Remove any diskettes from the diskette drive and turn off the power.
2. Insert a ROMPaq diskette into the diskette drive.
3. Turn on power to the system.
4. If no ROMPaq diskette is found, you will be prompted to insert one and restart the computer.
5. If a setup password has been established, the Caps Lock light will turn on and you will be prompted to enter the password.
6. Enter the setup password.
7. If the system successfully starts from the diskette and successfully reprograms the ROM, then the three keyboard lights will turn on. A “rising tone” series of beeps also signals successful completion.

To validate that the ROM flash was successful, complete the following steps:

1. Insert a valid ROMPaq diskette in the diskette drive.
2. Turn off power to the system.
3. Turn power on to the system to reflash the ROM.
4. If the ROM flash is successful, all three keyboard LEDs will light up, and you will hear a rising tone series of beeps.
5. Remove the diskette and turn the power off, then on to restart the computer.

The following table lists the various keyboard light combinations used by the Boot Block ROM, as well as the meaning and action associated with each combination.

Keyboard Light Combinations Used by Boot Block ROM

Failsafe Boot Block Mode	Keyboard LED Color	Keyboard LED Activity	State/Message
Num Lock	Green	On	ROMPaq diskette not present, is bad, or drive not ready.*
Caps Lock	Green	On	Enter password.*
Num, Caps, Scroll Lock	Green	Turn on and off 2 times (accompanied by 1 long and 3 short beeps)	ROM flash failed.*
Num, Caps, Scroll Lock	Green	On	Boot Block ROM Flash successful. Turn power off, then on to reboot.

✎ Diagnostic lights do not flash on USB keyboards.

Replicating Your Setup

This procedure gives an administrator the ability to easily copy one setup configuration to other computers of the same model. This allows for faster, more consistent configuration of multiple computers. To replicate your setup:

1. Access the Computer Setup Utilities (F10) menu.
2. Click **File > Save to Diskette.** Follow the instructions on the screen.

✎ This requires an internal diskette drive or a portable, external diskette drive.

3. To replicate the configuration, click **File > Restore** from Diskette, and follow the instructions on the screen.

Altiris eXpress, System Software Manager, and PC Transplant make it easy to replicate the configuration and custom settings of one PC and copy it to one or more PCs. For more information, visit http://www.compaq.com/easydeploy.

Dual-State Power Button

With Advanced Configuration and Power Interface (ACPI) enabled for Windows 98, Windows 2000, Windows Millennium, and Windows XP, the power button can function either as an on/off switch or as a suspend button. The suspend feature does not completely turn off power, but instead causes the computer to enter a low-power standby. This allows you to quickly power down without closing applications and to quickly return to the same operational state without any data loss.

To change the power button's configuration, complete the following steps:

1. In Windows 2000, left click on the **Start Button,** then select **Settings > Control Panel > Power Options.**

   In Windows XP, left click on the **Start Button,** then select **Control Panel > Performance and Maintenance > Power Options.**

2. In the **Power Options Properties,** select the **Advanced** tab.
3. In the Power buttons section, select the desired power button setting.

After configuring the power button to function as a suspend button, press the power button to put the system in a very low power state (suspend). Press the button again to quickly bring the system out of suspend to full power status. To completely turn off all power to the system, press and hold the power button for four seconds.

Power Management

Power Management is a feature that saves energy by shutting down certain components of the computer when they are not in use, saving energy without having to shut down the computer.

With Advanced Configuration and Power Interface (ACPI) enabled for Windows 98, Windows 2000, Windows Millennium, and Windows XP, timeouts (the period of inactivity allowed before shutting down these components) can be enabled, customized, or disabled using the operating system.

1. In Windows 2000, left click on the **Start Button,** then select **Settings > Control Panel > Power Options.**

   In Windows XP, left click on the **Start Button,** then select **Control Panel > Performance and Maintenance > Power Options.**
2. In the **Power Options Properties,** select the **Power Schemes** tab.
3. Select the desired power scheme settings.

Use Display Properties to establish, modify, or disable Power Management settings for the monitor. To access Display Properties, right click on the **Windows Desktop,** then choose **Properties.**

World Wide Web Site

HP engineers rigorously test and debug software developed by HP and third-party suppliers, and develop operating system specific support software, to ensure the highest level of performance, compatibility, and reliability for HP computers.

When making the transition to new or revised operating systems, it is important to implement the support software designed for that operating system. If you plan to run a version of Microsoft Windows that is different from the version included with your computer, you must install corresponding device drivers and utilities to ensure that all features are supported and functioning properly.

HP has made the task of locating, accessing, evaluating, and installing the latest support software easier. You can download the software from http://www.compaq.com.

The Web site contains the latest device drivers, utilities, and flashable ROM images needed to run the latest Microsoft Windows operating system on your HP computer.

Building Blocks and Partners

HP management solutions are based on industry standards, including DMI 2.0, Web-Based Enterprise Management, Intel's Wired for Management (WfM), SNMP, and PXE (preboot execution environment) technologies. Microsoft, Intel, Altiris, and other industry leaders work closely with HP to integrate their management solutions with HP products and initiatives to provide HP customers with leading-edge Intelligent Manageability solutions for personal systems. For more information, visit http://www.compaq.com/easydeploy.

Desktop Management Interface (DMI)

The Desktop Management Task Force (DMTF) is an industry body created in 1992 with the goal of standardizing systems manageability. DMTF established the Desktop Management Interface (DMI) framework to standardize access to PC configuration data. HP, as a Steering Committee and Technical Committee member of the DMTF, delivers hardware and software instrumentation that supports the DMI standard.

For more information on configuring the DMI software, refer to the *Intelligent Manageability Guide* help file.

Wired for Management

Intel's Wired for Management initiative is focused on reducing the support and administration cost of Intel architecture-based systems without compromising flexibility and performance. The Wired for Management guidelines provide a baseline set of building blocks that HP utilizes in Intelligent Manageability to provide standardized management of desktop inventories, remote system configuration, off-hours maintenance, and next generation power management. But HP does not stop with these baseline features. Additional capabilities have been incorporated into Intelligent Manageability to provide an extensive solution for managing networked computing environments.

Wired for Management technologies include:

- Desktop Management Interface (DMI) 2.0
- Remote System Installation
- Remote Wakeup and Remote Shutdown
- ACPI-Ready Hardware
- SMBIOS
- Pre-boot Execution (PXE) support

Asset Tracking and Security

Compaq AssetControl features incorporated into the computer provide key asset tracking data that can be managed using HP Insight Manager products and Management Solutions Partners products. Seamless, automatic integration between AssetControl features and these products enables you to choose the management tool that is best suited to your environment and to leverage your investment in existing tools.

HP computers are manufactured with the hardware and firmware required to fully support the DMI 2.0 standard.

HP also offers several solutions for controlling access to valuable components and information. Security features such as the Smart Cover Sensor and the Smart Cover Lock, available on select models, help to prevent unauthorized access to the internal components of the personal computer. By disabling parallel, serial, or USB ports, or by disabling removable media boot capability, you can protect valuable data assets. Memory Change and Smart Cover Sensor alerts can be automatically forwarded to HP Insight Manager products to deliver proactive notification of tampering with a computer's internal components.

✎ The Smart Cover Sensor and the Smart Cover Lock are available as options on select systems.

Use the following utilities to manage security settings on your HP computer:

- Locally, using the Computer Setup Utilities. See the *Computer Setup (F10) Utility Guide* included with the computer for additional information and instructions on using the Computer Setup Utilities.
- Remotely, using System Software Manager. This software enables the secure, consistent deployment and control of security settings from a simple command-line utility.

The following table and sections refer to managing security features of your computer locally through the Computer Setup Utilities (F10).

Security Features Overview

Feature	Purpose	How It Is Established
Removable Media Boot Control	Prevents booting from the removable media drives.	From the Computer Setup Utilities (F10) menu.
Serial, Parallel, USB, or Infrared Interface Control	Prevents transfer of data through the integrated serial, parallel, USB (universal serial bus), or infrared interface.	From the Computer Setup Utilities (F10) menu.
Power-On Password	Prevents use of the computer until the password is entered. This can apply to both initial system startup and restarts.	From the Computer Setup Utilities (F10) menu.
Setup Password	Prevents reconfiguration of the computer (use of the Computer Setup Utilities) until the password is entered.	From the Computer Setup Utilities (F10) menu.
Network Server Mode	Provides unique security features for computers being used as servers.	From the Computer Setup Utilities (F10) menu.
DriveLock	Prevents unauthorized access to the data on specific hard drives. This feature is available on select models only.	From the Computer Setup Utilities (F10) menu.
Smart Cover Sensor	Indicates that computer cover or side panel has been removed. Can be set to require the setup password to restart the computer, after the cover or side panel has been removed. Refer to the *Hardware Reference Guide* on the *Documentation Library* CD for more information about this feature.	From the Computer Setup Utilities (F10) menu.

Security Features Overview *(Continued)*

Feature	Purpose	How It Is Established
Master Boot Record Security	May prevent unintentional or malicious changes to the Master Boot Record of the current bootable disk, and provides a means of recovering the "last known good" MBR.	From the Computer Setup Utilities (F10) menu.
Memory Change Alerts	Detects when memory modules have been added, moved, or removed; notifies user and system administrator.	For information on enabling Memory Change Alerts, refer to the online *Intelligent Manageability Guide*.
Ownership Tag	Displays ownership information, as defined by the system administrator, during system startup (protected by setup password).	From the Computer Setup Utilities (F10) menu.
Cable Lock Provision	Inhibits access to the interior of the computer to prevent unwanted configuration changes or component removal. Can also be used to secure the computer to a fixed object to prevent theft.	Install a cable lock to secure the computer to a fixed object.
Security Loop Provision	Inhibits access to the interior of the computer to prevent unwanted configuration changes or component removal.	Install a lock in the security loop to prevent unwanted configuration changes or component removal.

✎ For more information about Computer Setup, see the *Computer Setup (F10) Utility Guide*. Support for security features may vary depending on your specific computer configuration.

Password Security

The power-on password prevents unauthorized use of the computer by requiring entry of a password to access applications or data each time the computer is turned on or restarted. The setup password specifically prevents unauthorized access to Computer Setup, and can also be used as an override to the power-on password. That is, when prompted for the power-on password, entering the setup password instead will allow access to the computer.

A network-wide setup password can be established to enable the system administrator to log in to all network systems to perform maintenance without having to know the power-on password, even if one has been established.

Establishing a Setup Password Using Computer Setup

Establishing a setup password through Computer Setup prevents reconfiguration of the computer (use of the Computer Setup (F10) utility) until the password is entered.

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart the Computer.**
2. When the F10 Setup message appears in the lower-right corner of the screen, press the **F10** key. Press **Enter** to bypass the title screen, if necessary.

✎ If you do not press the **F10** key while the message is displayed, you must restart the computer to access the utility.

3. Select **Security,** then select **Setup Password** and follow the instructions on the screen.
4. Before exiting, click **File > Save Changes** and **Exit.**

Establishing a Power-On Password Using Computer Setup

Establishing a power-on password through Computer Setup prevents access to the computer when power is turned on, unless the password is entered. When a power-on password is set, Computer Setup presents Password Options under the Security menu. The password options include Network Server Mode and Password Prompt on Warm Boot.

When Network Server Mode is disabled, the password must be entered each time the computer is turned on when the key icon appears on the monitor. When Password Prompt on Warm Boot is enabled, the password must also be entered each time the computer is rebooted. When Network Server Mode is enabled, the password prompt is not presented during POST, but any attached PS/2 keyboard will remain locked until the user enters the power-on password.

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart the Computer.**
2. When the F10 Setup message appears in the lower-right corner of the screen, press the **F10** key. Press **Enter** to bypass the title screen, if necessary.

✎ If you do not press the **F10** key while the message is displayed, you must restart the computer to access the utility.

3. Select **Security,** then **Power-On Password** and follow the instructions on the screen.
4. Before exiting, click **File > Save Changes** and **Exit.**

Entering a Power-On Password

To enter a power-on password, complete the following steps:

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart the Computer.**
2. When the key icon appears on the monitor, type your current password, then press **Enter.**

✎ Type carefully; for security reasons, the characters you type do not appear on the screen.

If you enter the password incorrectly, a broken key icon appears. Try again. After three unsuccessful tries, you must turn off the computer, then turn it on again before you can continue.

Entering a Setup Password

If a setup password has been established on the computer, you will be prompted to enter it each time you run Computer Setup.

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart the Computer.**
2. When the F10 = Setup message appears in the lower-right corner of the screen, press the **F10** key.

✎ If you do not press the **F10** key while the message is displayed, you must restart the computer to access the utility.

3. When the key icon appears on the monitor, type the setup password, then press the **Enter** key.

✎ Type carefully; for security reasons, the characters you type do not appear on the screen.

If you enter the password incorrectly, a broken key icon appears. Try again. After three unsuccessful tries, you must turn off the computer, then turn it on again before you can continue.

Changing a Power-On or Setup Password

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart the Computer.** To change the setup password, run **Computer Setup.**
2. When the key icon appears, type your current password, a slash (/) or alternate delimiter character, your new password, another slash (/) or alternate delimiter character, and your new password again as shown:
   current password/new password/new password

✎ Type carefully; for security reasons, the characters you type do not appear on the screen.

3. Press the **Enter** key.

The new password takes effect the next time you turn on the computer.

✎ Refer to the "National Keyboard Delimiter Characters" section in this chapter for information about the alternate delimiter characters.
The power-on password and setup password may also be changed using the Security options in Computer Setup.

Deleting a Power-On or Setup Password

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart the Computer.** To delete the setup password, run **Computer Setup.**
2. When the key icon appears, type your current password followed by a slash (/) or alternate delimiter character as shown: **current password/**
3. Press the **Enter** key.

✎ Refer to "National Keyboard Delimiter Characters" for information about the alternate delimiter characters. The power-on password and setup password may also be changed using the Security options in Computer Setup.

National Keyboard Delimiter Characters

Each keyboard is designed to meet country-specific requirements. The syntax and keys that you use for changing or deleting your password depend on the keyboard that came with your computer.

National Keyboard Delimiter Characters

Arabic	/	Greek	-	Russian	/
Belgian	=	Hebrew	.	Slovakian	-
BHCSY*	-	Hungarian	-	Spanish	-
Brazilian	/	Italian	-	Swedish/Finnish	/
Chinese	/	Japanese	/	Swiss	-
Czech	-	Korean	/	Taiwanese	/
Danish	-	Latin American	-	Thai	/
French	!	Norwegian	-	Turkish	.
French Canadian	é	Polish	-	U.K. English	/
German	-	Portuguese	-	U.S. English	/

* For Bosnia-Herzegovina, Croatia, Slovenia, and Yugoslavia

Clearing Passwords

If you forget your password, you cannot access the computer. Refer to the *Troubleshooting Guide* for instructions on clearing passwords.

Network Server Mode

Network Server Mode provides unique security features for computers being used as servers. It is only available when a power-on password has been set in Computer Setup. When the Network Server Mode is enabled, the power-on password is not required to boot the hard drive, and a keyboard is not required to be attached to the system. If a PS/2 keyboard is present, it will be locked until the user enters the power-on password. If a USB keboard is present, it will remain usable by default. To prevent USB keyboard access after the operating system has loaded, a user must hide the USB Port under the Device Security option of Computer Setup's Security menu. When used in conjunction with the Computer Setup After Power Loss power-on option, Network Server Mode permits the "server" to automatically reboot after a power interruption without user intervention. While Network Server Mode is enabled, the power-on password must be entered to boot the removable media (e.g. diskettes) or removable devices (e.g. USB flash devices).

DriveLock

DriveLock is a security feature that prevents unauthorized access to the data on specific hard drives. DriveLock has been implemented as an extension to Computer Setup. It is only available on certain systems and only when DriveLock-capable hard drives are detected.

DriveLock is intended for HP customers for whom data security is the paramount concern. For such customers, the cost of the hard drive and the loss of the data stored on it is inconsequential when compared with the damage that could result from unauthorized access to its contents. In order to balance this level of security with the practical need to accomodate a forgotten password, DriveLock employs a two-password security scheme. One password is intended to be set and used by a system administrator while the other is typically set and used by the end-user. There is no "back-door" that can be used to unlock the drive if both passwords are forgotten. Therefore, DriveLock is most safely used when the data contained on the hard drive is replicated on a corporate information system or is regularly backed up.

In the event that both DriveLock passwords are lost, the hard drive is rendered unusable. For any user who does not fit the previously defined customer profile, this may be an unacceptable risk. For users who do fit the customer profile, it may be a tolerable risk given the nature of the data stored on the hard drive.

Using DriveLock

The DriveLock option appears under the Security menu in Computer Setup. The user is presented with options to set the master password or to enable DriveLock. A user password must be provided in order to enable DriveLock. Since the initial configuration of DriveLock is typically performed by a system administrator, a master password should be set first. HP encourages system administrators to set a master password whether they plan to enable DriveLock or keep it disabled. This will give the administrator the ability to modify DriveLock settings if the drive is locked in the future. Once the master password is set, the system administrator may enable DriveLock or choose to keep it disabled.

If a locked hard drive is present, POST will require a password to unlock the device. If a power-on password is set and it matches the device's user password, POST will not prompt the user to re-enter the password. Otherwise, the user will be prompted to enter a DriveLock password. Either the master or the user password may be used. Users will have two attempts to enter a correct password. If neither attempt succeeds, POST will continue but the data on the drive will remain inaccessible.

DriveLock Applications

The most practical use of the DriveLock security feature is in a corporate environment where a system administrator provides users with multibay hard drives for use in some computers. The system administrator would be responsible for configuring the multibay hard drive which would involve, among other things, setting the DriveLock master password. In the event that the user forgets the user password or the equipment is passed on to another employee, the master password can always be used to reset the user password and regain access to the hard drive.

HP recommends that corporate system administrators who choose to enable DriveLock also establish a corporate policy for setting and maintaing master passwords. This should be done to prevent a situation where an employee intentionally or unintentionally sets both DriveLock passwords before leaving the company. In such a scenario, the hard drive would be rendered unusable and require replacement. Likewise, by not setting a master password, system administrators may find themselves locked out of a hard drive and unable to perform routine checks for unauthorized software, other asset control functions, and support.

For users with less stringent security requirements, HP does not recommend enabling DriveLock. Users in this category include personal users or users who do not maintain sensitive data on their hard drives as a common practice. For these users, the potential loss of a hard drive resulting from forgetting both passwords is much greater than the value of the data DriveLock has been designed to protect. Access to Computer Setup and DriveLock can be restricted through the Setup password. By specifying a Setup password and not giving it to end users, system administrators are able to restrict users from enabling DriveLock.

Smart Cover Sensor

Smart Cover Sensor, available on select models, is a combination of hardware and software technology that can alert you when the computer cover or side panel has been removed. There are three levels of protection, as described in the following table.

Smart Cover Sensor Protection Levels

Level	Setting	Description
Level 0	Disabled	Smart Cover Sensor is disabled (default).
Level 1	Notify User	When the computer is restarted, the screen displays a message indicating that the computer cover or side panel has been removed.
Level 2	Setup Password	When the computer is restarted, the screen displays a message indicating that the computer cover or side panel has been removed. You must enter the setup password to continue.

✎ These settings can be changed using Computer Setup. For more information about Computer Setup, see the *Computer Setup (F10) Utility Guide.*

Setting the Smart Cover Sensor Protection Level

To set the Smart Cover Sensor protection level, complete the following steps:

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart the Computer.**
2. When the F10 Setup message appears in the lower-right corner of the screen, press the **F10** key. Press **Enter** to bypass the title screen, if necessary.

✎ If you do not press the **F10** key while the message is displayed, you must restart the computer to access the utility.

3. Select **Security,** then **Smart Cover,** and follow the instructions on the screen.
4. Before exiting, click **File > Save Changes** and **Exit.**

Smart Cover Lock

The Smart Cover Lock is a software-controllable cover lock featured on select HP computers. This lock prevents unauthorized access to the internal components. Computers ship with the Smart Cover Lock in the unlocked position.

△ **CAUTION:** For maximum cover lock security, be sure to establish a setup password. The setup password prevents unauthorized access to the Computer Setup utility.

✎ The Smart Cover Lock is available as an option on select systems.

Locking the Smart Cover Lock

To activate and lock the Smart Cover Lock, complete the following steps:

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart the Computer.**
2. When the F10 Setup message appears in the lower-right corner of the screen, press the **F10** key. Press **Enter** to bypass the title screen, if necessary.

✎ If you do not press the **F10** key while the message is displayed, you must restart the computer to access the utility.

3. Select **Security,** then select **Smart Cover** and the **Locked** option.
4. Before exiting, click **File > Save Changes** and **Exit.**

Unlocking the Smart Cover Lock

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart the Computer.**
2. When the F10 Setup message appears in the lower-right corner of the screen, press the **F10** key. Press **Enter** to bypass the title screen, if necessary.

✎ If you do not press the **F10** key while the message is displayed, you must restart the computer to access the utility.

3. Select **Security > Smart Cover > Unlocked.**
4. Before exiting, click **File > Save Changes** and **Exit.**

Using the Smart Cover FailSafe Key

If you enable the Smart Cover Lock and cannot enter your password to disable the lock, you will need a Smart Cover FailSafe Key to open the computer cover. You will need the key in any of the following circumstances:

- Power outage
- Startup failure
- PC component failure (such as processor or power supply)
- Forgotten password

⚠ **CAUTION:** The Smart Cover FailSafe Key is a specialized tool available from HP. Be prepared; order this key before you need one at an authorized reseller or service provider (order PN 166527-001 for the wrench-style key or PN 166527-002 for the screwdriver bit key).

To obtain the FailSafe Key, do any one of the following:

- Contact your authorized HP reseller or service provider.
- Visit http://www.compaq.com for ordering information.
- Call the appropriate number listed in the warranty.

For more information about using the Smart Cover FailSafe Key, consult the *Hardware Reference Guide.*

Master Boot Record Security

The Master Boot Record (MBR) contains information needed to successfully boot from a disk and to access the data stored on the disk. Master Boot Record Security may prevent unintentional or malicious changes to the MBR, such as those caused by some computer viruses or by the incorrect use of certain disk utilities. It also allows you to recover the "last known good" MBR, should changes to the MBR be detected when the system is restarted.

To enable MBR Security, complete the following steps:

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart the Computer.**
2. When the F10 Setup message appears in the lower-right corner of the screen, press the **F10** key. Press **Enter** to bypass the title screen, if necessary.

✎ If you do not press the **F10** key while the message is displayed, you must restart the computer to access the utility.

3. Select **Security > Master Boot Record Security > Enabled.**
4. Select **Security > Save Master Boot Record.**
5. Before exiting, click **File > Save Changes** and **Exit.**

When MBR Security is enabled, the BIOS prevents any changes being made to the MBR of the current bootable disk while in MS-DOS or Windows Safe Mode.

✎ Most operating systems control access to the MBR of the current bootable disk; the BIOS cannot prevent changes that may occur while the operating system is running.

Each time the computer is turned on or restarted, the BIOS compares the MBR of the current bootable disk to the previously saved MBR. If changes are detected and if the current bootable disk is the same disk from which the MBR was previously saved, the following message is displayed:

> 1999—Master Boot Record has changed.
>
> Press any key to enter Setup to configure MBR Security.

Upon entering Computer Setup, you must

- Save the MBR of the current bootable disk;
- Restore the previously saved MBR; or
- Disable the MBR Security feature.

You must know the setup password, if one exists.

If changes are detected and if the current bootable disk is **not** the same disk from which the MBR was previously saved, the following message is displayed:

> 2000—Master Boot Record Hard Drive has changed.
>
> Press any key to enter Setup to configure MBR Security.

Upon entering Computer Setup, you must

- Save the MBR of the current bootable disk; or
- Disable the MBR Security feature.

You must know the setup password, if one exists.

In the unlikely event that the previously saved MBR has been corrupted, the following message is displayed:

> 1998—Master Boot Record has been lost.
>
> Press any key to enter Setup to configure MBR Security.

Upon entering Computer Setup, you must

- Save the MBR of the current bootable disk; or
- Disable the MBR Security feature.

You must know the setup password, if one exists.

Before You Partition or Format the Current Bootable Disk

Ensure that MBR Security is disabled before you change partitioning or formatting of the current bootable disk. Some disk utilities, such as FDISK and FORMAT, attempt to update the MBR. If MBR Security is enabled when you change partitioning or formatting of the disk, you may receive error messages from the disk utility or a warning from MBR Security the next time the computer is turned on or restarted. To disable MBR Security, complete the following steps:

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart the Computer.**
2. When the F10 Setup message appears in the lower-right corner of the screen, press the **F10** key. Press **Enter** to bypass the title screen, if necessary.

✎ If you do not press the **F10** key while the message is displayed, you must restart the computer to access the utility.

3. Select **Security > Master Boot Record Security > Disabled.**
4. Before exiting, click **File > Save Changes** and **Exit.**

Cable Lock Provision

The rear panel of the computer accommodates a cable lock so that the computer can be physically secured to a work area.

For illustrated instructions, please see the *Hardware Reference Guide* on the *Documentation Library* CD.

Fingerprint Identification Technology

Eliminating the need to enter user passwords, HP Fingerprint Identification Technology tightens network security, simplifies the login process, and reduces the costs associated with managing corporate networks. Affordably priced, it is not just for high-tech, high-security organizations anymore.

✎ Support for Fingerprint Identification Technology varies by model.

For more information, visit:
http://www.compaq.com/products/quickspecs/10690_na/10690_na.html

Fault Notification and Recovery

Fault Notification and Recovery features combine innovative hardware and software technology to prevent the loss of critical data and minimize unplanned downtime.

When a fault occurs, the computer displays a Local Alert message containing a description of the fault and any recommended actions. You can then view current system health by using the HP Insight Management Agent. If the computer is connected to a network managed by an HP Insight Manager product or other management products from Compaq Management Solutions Partners, the computer also sends a fault notice to the network management application.

Drive Protection System

The Drive Protection System (DPS) is a diagnostic tool built into the hard drives installed in select HP computers. DPS is designed to help diagnose problems that might result in unwarranted hard drive replacement.

When HP computers are built, each installed hard drive is tested using DPS, and a permanent record of key information is written onto the drive. Each time DPS is run, test results are written to the hard drive. Your service provider can use this information to help diagnose conditions that caused you to run the DPS software. Refer to the *Troubleshooting Guide* for instructions on using DPS.

Ultra ATA Integrity Monitoring

Ultra ATA Integrity Monitoring monitors the integrity of data as it is transferred between an Ultra ATA hard drive and the system's core logic. If the computer detects an abnormal number of transmission errors, the computer displays a Local Alert message with recommended actions.

Surge-Tolerant Power Supply

An integrated surge-tolerant power supply provides greater reliability when the computer is hit with an unpredictable power surge. This power supply is rated to withstand a power surge of up to 2000 volts without incurring any system downtime or data loss.

Thermal Sensor

The thermal sensor is a hardware and software feature that tracks the internal temperature of the computer. This feature displays a warning message when the normal range is exceeded, which gives you time to take action before internal components are damaged or data is lost.

Index